IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No. :	**10/803,945**	Confirmation No. 7176
Applicant :	K. SHIMOOKA et al.	
Filed :	March 19, 2004	
Title :	DATA PROTECTING APPARATUS AND METHOD, AND COMPUTER SYSTEM	
TC/AU :	2818	
Examiner :	TBA	
Docket No. :	TSM-37	
Customer No.:	24956	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION TO MAKE SPECIAL UNDER 37 CFR §1.102(d) (MPEP §708.02(VIII))

Sir:

The Applicants petition the Commissioner to make the above-identified application special in accordance with 37 CFR §1.102(d). In support of this Petition, pursuant to MPEP § 708.02(VIII), Applicants state the following.

(A) REQUIRED FEE

This Petition is accompanied by the fee set forth in 37 CFR § 1.117(h). A Credit Card Payment Form in the amount of $130 accompanies this Petition in satisfaction of the fee. The Commissioner is hereby authorized to charge any additional payment due, or to credit any overpayment, to Deposit Account No. 50-1417.

(B) ALL CLAIMS DIRECTED TO A SINGLE INVENTION

All the pending claims of the application, claims 1-7, 9-17, and 19-20, are directed to a single invention. If the Office determines that all claims in the application are not directed to a single invention, Applicant will make election without traverse as a prerequisite to the grant of special status.

The claimed invention is generally directed to an intrusion detection and data protection system and method for a computer system. In a first aspect, as set forth in independent claim 1, the invention is a data protection apparatus for protecting data in a storage volume in a computer system. The computer system includes the storage volume assigned for storing data, a computer for reading and writing data from and to the storage volume, and a storage control unit for controlling communication between the computer and the storage volume. The data protection apparatus includes an event detection unit for detecting an event occurrence, and a path disconnection unit for instructing the storage control unit to stop communication between the computer and the storage volume, when the event detection unit detects an event.

Additionally, as set forth in independent claim 4, the invention is a data protection method for protecting data in a storage volume in a computer system, with the computer system including the storage volume assigned for storing data, a computer for reading and writing data from and to the storage volume, and a storage control unit for controlling communication between the computer and the storage volume. The data protection method includes detecting an event occurrence, and disconnecting a path to stop communication between the computer and the storage volume when the event is detected.

Furthermore, as set forth in independent claim 5, the invention is a program for making an information processing apparatus perform data protection of a storage volume in a computer system. The computer system includes the storage volume assigned for storing data, a computer for reading and writing data from and to the storage volume, and a storage control unit for controlling communication between the computer and the storage volume. The program makes the information processing apparatus perform processes of detecting an event occurrence, and disconnecting a path to stop communication between the computer and the storage volume after the event is detected.

In addition, as set forth in independent claim 6, the invention is a computer system that includes a storage volume assigned for storing data, a computer for reading and writing data from and to the storage volume, a storage control unit for controlling communication between the computer and the storage volume, and a data protection apparatus for protecting data in the storage volume. The data protection apparatus includes an event detection unit for detecting an event occurrence, and a path disconnection unit for instructing the storage control unit to stop communication between the computer and the storage volume when the event detection unit detects an event.

Also, as set forth in independent claim 7, the invention is a data protection apparatus for protecting data in a storage volume in a computer system. The computer system includes the storage volume assigned for storing data, a replicated volume assigned for storing data duplicated from the storage volume, and a storage control unit for controlling data transfer from the storage volume to the replicated volume. The data protection apparatus includes an event detection unit for detecting an event occurrence, and a replication stopping unit for instructing the storage control unit to stop data transfer from the storage volume to the replicated volume when the event detection unit detects an event. The computer system further includes a computer for reading and writing data from and to the storage volume, and an illegal intrusion detection unit for detecting an illegal intrusion into the computer. The event detection unit is able to receive a detection of the illegal intrusion from the illegal intrusion detection unit. When the event detection unit receives the detection of the illegal intrusion, the replication stopping unit instructs the storage control unit to stop data transfer from the storage volume to the replicated volume.

In addition, as set forth in independent claim 10, the invention is directed to a data protection method for protecting data in a storage volume in a computer system. The computer system includes the storage volume assigned for storing data, a computer for reading and writing data from and to the storage volume, a replicated volume assigned for storing data duplicated from the storage volume, and a storage control unit for controlling data transfer from the storage volume to the replicated volume. The data protection method includes detecting an intrusion into the computer, and instructing the storage control unit to stop data transfer from the storage volume to the replicated volume, when the intrusion is detected.

Furthermore, as set forth in independent claim 11, the invention is a program for making an information processing apparatus perform data protection of a storage volume in a computer system. The computer system includes the storage volume assigned for storing data, a computer for reading and writing data from and to the storage volume, a replicated volume assigned for storing data duplicated from the storage volume, and a storage control unit for controlling data transfer from the storage volume to the replicated volume. The program makes the information processing apparatus perform processes of detecting that an intrusion into the computer has occurred, and instructing the storage control unit to stop data transfer from the storage volume to the replicated volume when the intrusion is detected.

Also, as set forth in independent claim 14, the invention is a computer system including a storage volume assigned for storing data, a replicated volume assigned for storing data duplicated from the storage volume, a storage control unit for controlling data transfer from the storage volume to the replicated volume, and a data protection apparatus for protecting data in the storage volume. The data protection apparatus includes an event detection unit for detecting an event occurrence, and a replication stopping unit for instructing the storage control unit to stop data transfer from the storage volume to the replicated volume, when the event detection unit detects an event. The computer system further includes an alteration detection unit that reads given data in the plurality of replicated volumes to detect respective differences between the given data. The event detected by the event detection unit is a detection result of the differences between the given data, with the detection result being received from the alteration detection unit.

Finally, as set forth in independent claim 20, the invention is a computer system including a storage apparatus including a storage volume assigned for storing data, a replicated volume assigned for storing data duplicated from the storage volume, a host computer for reading and writing data from and to the storage volume, a storage control unit for controlling communication between the host computer and the storage volume, and a data protection apparatus for protecting data in the storage volume. The host computer detects an illegal intrusion and sends a notification of the detected illegal intrusion to the data protection apparatus. The data protection apparatus receives the notification and gives the storage control unit an instruction to disconnect a path to stop communication between the computer and the storage volume. The storage control unit, receiving the instruction, rejects access from outside to the storage volume of the storage apparatus.

(C) PRE-EXMINATION SEARCH

A careful and thorough pre-examination search has been conducted, directed to the invention as claimed. The pre-examination search was conducted in the following areas:

Class	Subclass
365	222
709	224
711	162, 163
713	200, 201

Furthermore, a keyword search was conducted on the USPTO's EAST database. Additionally, a literature search was also conducted for relevant non-patent documents using the Association for Computing Machinery online databases. In addition, a search for foreign patent documents was conducted on the ESPACENET databases.

(D) DOCUMENTS DEVELOPED BY THE PRE-EXAMINATION SEARCH

Of the documents reviewed during the search, those deemed to be most closely related to the subject matter encompassed by the claims are listed below. These documents were made of record in the present application by the Information Disclosure Statement filed January 13, 2005.

Patent/App. No.	Inventor(s)
US 5918008	Togawa, Yoshifusa et al.
US 20010007120	Makita, Satoshi
US 20040010732	Oka, Nobuyuki
US 20040025044	Day, Christopher W.
US 20040078636	Suzaki, Kuniyasu
US 20040117401	Miyata, Kenichi et al.

Patent/App. No.	**Inventor(s)**
US 20040143761	Mendonca, John et al.

Additionally, the following document was made of record in the present application by the Information Disclosure Statement filed June 4, 2004.

Publication

6.3.3. "Intrusion Detection Systems", Introduction to Network Management for Beginners, in Foundation for Multimedia Communications, Network Management Section, (online), May 15, 2002.

Because all of the above-listed documents are already of record in the present application, in accordance with MPEP § 708.02(VIII)(D), additional copies of these documents have not been submitted with this Petition.

(E) DETAILED DISCUSSION OF THE REFERENCES

A discussion of each the above-listed documents is set forth below, pointing out, with the particularity required by 37 CFR 1.111 (b) and (c), how the claimed subject matter is patentable over the teachings of the above-listed documents.

The patent to Togawa et al., US 5918008, shows a storage device having a function for coping with a computer virus. The device includes a virus checker that detects whether a file stored on a disk is infected with a virus with reference to an infection management table. When a judging means has judged that a file is infected with a virus, a prohibiting means prohibits use of the file. (See, e.g., Abstract and column 2, lines 23-36.) Thus, Togawa does not teach the present invention, wherein a path disconnection unit is included for instructing a storage control unit to stop communication between a computer and a storage volume when an event detection unit detects an event, as set forth in claims 1 and 6. Nor does Togawa teach instructing a storage control unit to stop data transfer from a storage volume to a replicated volume when an intrusion is detected, as set forth in claims 7, 10, and 11. Additionally, Togawa does not teach a method or program in which a path is disconnected to stop communication between a computer and a storage volume when an event is detected, as set forth in claims 4, 5, and 20. Also, Togawa does not teach an alteration detection unit as set forth in claim 14. Accordingly, independent claims 1, 4, 5, 6, 7, 10, 11, 14, and 20 are patentable over Togawa.

The published US patent application to Makita, US 20010007120, shows a storage device connected to a host computer. The storage device includes a virus check unit so that it is unnecessary for the host computer to perform a virus check, thus reducing a processing load imposed on the host computer. The virus check unit performs a virus check at a time of recording a file on, or reading out a file from a recording medium, or based on a frequency of accesses from the one of the host computers to the recording medium. When a virus is discovered, storing the information on the recording medium is halted, and the host computer is notified that the virus is discovered. (See, e.g., Abstract and paragraphs [0062]-[0063] and [0172]-[0176].) However, Makita does not teach the present invention, wherein a path disconnection unit is included for instructing a storage control unit to stop communication between a computer and a storage volume when an event detection unit detects an event, as set forth in claims 1 and 6. Nor does Makita teach instructing a storage control unit to stop data transfer from a storage volume to a replicated volume when an intrusion is detected, as set forth in claims 7, 10, and 11. Additionally, Makita does not teach a method or program in which a path is disconnected to stop communication between a computer and a storage volume when an event is detected, as set forth in claims 4, 5, and 20. Also, Makita does not teach an alteration detection unit as set forth in claim 14. Accordingly, independent claims 1, 4, 5, 6, 7, 10, 11, 14, and 20 are patentable over Makita.

The published US patent application to Oka, US 20040010732, shows a backup method and storage control device in which performing the backup includes: having the storage control device allocate a specified number of generations of the backup volume in the storage device for the copy volume; instructing the storage device to split a pair of volumes; executing a virus check on the copy volume of the pair; copying the contents of the checked copy volume to the backup volume as a most recent generation backup for the copy volume if no virus is detected by the virus check; updating the generations in the backup volume for generations prior to the most recent generation; and instructing the storage device to re-link the split pair. If a virus is detected as a result of a virus check based on virus definition update scheduling information, information looked-up or updated from the generation/backup/restore target management module is used to perform a restore while the system is in a degraded operating state in which an attribute indicating unavailability is applied to the primary volume and the copy volume. Alternatively, the system can be stopped. (See, e.g., Abstract, and paragraphs [0008], [0021], [0039]-[0046], and [0057].) However, Oka does not teach the present invention, since changing a volume attribute to indicate unavailability does not necessarily stop communication between a computer and a storage volume, and does not disconnect the path. Thus, Oka does not teach a path disconnection unit for instructing a storage control unit to stop communication between a computer and a storage volume when an event detection unit detects an event, as set forth in claims 1 and 6. Nor does Oka teach a method or program in which a path is disconnected to stop communication between a computer and a storage volume when an event is detected, as set forth in claims 4, 5, and 20. Additionally, Oka does not teach replication stopping if an intrusion is detected in a computer, as set forth in claims 7, 10 and 11. Rather, Oka teaches stopping replication if a virus is detected in a file being replicated. Furthermore, Oka does not teach an alteration detection unit as set forth in claim 14. Accordingly, independent claims 1, 4, 5, 6, 7, 10, 11, 14, and 20 are patentable over Oka.

The published US patent application to Day, US 20040025044, shows an intrusion detection system that includes an anomaly detector and a classifier that can classify detected anomalous correlations based upon at least one configurable correlation metric. Where anomalous behavior has been classified as an event, individual clusters associated with the anomalous behavior can be further examined to determine whether an unauthorized network intrusion has occurred. (See, e.g., Abstract, and paragraphs [0035]-[0037].) However, Day does not teach the present invention, wherein a path disconnection unit is included for instructing a storage control unit to stop communication between a computer and a storage volume when an event detection unit detects an event, as set forth in claims 1 and 6. Nor does Day teach instructing a storage control unit to stop data transfer from a storage volume to a replicated volume when an intrusion is detected, as set forth in claims 7, 10, and 11. Additionally, Day does not teach a method or program in which a path is disconnected to stop communication between a computer and a storage volume when an event is detected, as set forth in claims 4, 5, and 20. Also, Day does not teach an alteration detection unit as set forth in claim 14. Accordingly, independent claims 1, 4, 5, 6, 7, 10, 11, 14, and 20 are patentable over Day.

The published US patent application to Suzaki, US 20040078636, shows a system with an input and output means for a computer system storage. The system includes a computer equipped with a first storage, a second storage that with respect to access speed operates at a higher speed than the first storage, and a processor. A virtual computer operating on the computer is included, and is equipped with a configuration that, when writing to the first storage, writes via a disk cache of a predetermined capacity. A data transfer path from the disk cache to a hard disk of the first storage is provided with a switch to control the flow of data, thereby controlling whether or not there are hard-disk rewrites. (See, e.g., Abstract, and paragraphs [0016]-[0018], [0031]-[0035].) Thus, Suzaki does not disconnect upon the occurrence of an event, and does not teach the present invention, wherein a path disconnection unit is included for instructing a storage control unit to stop communication between a computer and a storage volume when an event detection unit detects an event, as set forth in claims 1 and 6. Nor does Suzaki teach instructing a storage control unit to stop data transfer from a storage volume to a replicated volume when an intrusion is detected, as set forth in claims 7, 10, and 11. Additionally, Suzaki does not teach a method or program in which a path is disconnected to stop communication between a computer and a storage volume when an event is detected, as set forth in claims 4, 5, and 20. Also, Suzaki does not teach an alteration detection unit as set forth in claim 14. Accordingly, independent claims 1, 4, 5, 6, 7, 10, 11, 14, and 20 are patentable over Suzaki.

The published US patent application to Miyata, US 20040117401, shows an information processing system that includes a storage device system 16 that has an interface 161 for connection with a scan server 15 and a storage device 162 that contains a virus database. Scan server 15 includes an interface 151 for connection with network 12; a CPU 152; a memory 153 containing an OS 1531 and a virus scanner 1532; a network 154 in the scan server; and an interface 155 for connection with storage device system 16. CPU 152 executes virus scanner 1532, which compares a suspected file with associated patterns contained in virus database

1621. If a file is infected, the host CPU notifies a client that the file cannot be opened. (See, e.g., Abstract and paragraphs [0017]-[0019] and [0021].) Thus, Miyata does not disconnect upon the occurrence of an event, and does not teach the present invention, wherein a path disconnection unit is included for instructing a storage control unit to stop communication between a computer and a storage volume when an event detection unit detects an event, as set forth in claims 1 and 6. Nor does Miyata teach instructing a storage control unit to stop data transfer from a storage volume to a replicated volume when an intrusion is detected, as set forth in claims 7, 10, and 11. Additionally, Miyata does not teach a method or program in which a path is disconnected to stop communication between a computer and a storage volume when an event is detected, as set forth in claims 4, 5, and 20. Also, Miyata does not teach an alteration detection unit as set forth in claim 14. Accordingly, independent claims 1, 4, 5, 6, 7, 10, 11, 14, and 20 are patentable over Miyata.

The published US patent application to Mendonca, US 20040143761, is directed to a an intrusion detection system in a provisionable network. The system includes: evaluating the system security of the provisionable network; and applying a system lockdown in the provisionable network in accordance with the results of the evaluation. (See, e.g., Abstract and paragraphs [0014]-[0015].) However, Mendonca does not provide a path disconnection unit that is included for instructing a storage control unit to stop communication between a computer and a storage volume when an event detection unit detects an event, as set forth in claims 1 and 6. Nor does Mendonca teach instructing a storage control unit to stop data transfer from a storage volume to a replicated volume when an intrusion is detected, as set forth in claims 7, 10, and 11. Additionally, Mendonca does not teach a method or program in which a path is disconnected to stop communication between a computer and a storage volume when an event is detected, as set forth in claims 4, 5, and 20. Also, Mendonca does not teach an alteration detection unit as set forth in claim 14. Accordingly, independent claims 1, 4, 5, 6, 7, 10, 11, 14, and 20 are patentable over Mendonca.

The publication "Intrusion Detection Systems", provides a general discussion of intrusion detection systems for detecting in real time attempts to intrude into a network. Responses to a detected intrusion taught by the publication include displaying an alert notice, starting an external application, storing and studying the generated event, session cutoff, changing firewall rules and denying packets in question, and restoring the original contents of system file or registry which have been changed. (See, e.g., last two pages of the publication.) Thus, the publication does not teach the present invention, wherein a path disconnection unit is included for instructing a storage control unit to stop communication between a computer and a storage volume when an event detection unit detects an event, as set forth in claims 1 and 6. Nor does the publication teach instructing a storage control unit to stop data transfer from a storage volume to a replicated volume when an intrusion is detected, as set forth in claims 7, 10, and 11. Additionally, the publication does not teach a method or program in which a path is disconnected to stop communication between a computer and a storage volume when an event is detected, as set forth in claims 4, 5, and 20. Also, the publication does not teach an alteration detection unit as set forth in claim 14. Accordingly, independent claims 1, 4, 5, 6, 7, 10, 11, 14, and 20 are patentable over the publication.

CONCLUSION

The Applicants submit that the foregoing discussion demonstrates the patentability of independent claims 1, 4, 5, 6, 7, 10, 11, 14, and 20 over the closest-known prior art, taken either singly, or in combination. Accordingly, the requirements of 37 CFR §1.102(d) having been satisfied, the Applicants request that this Petition to Make Special be granted and that the application be examined according to prescribed procedures set forth in MPEP §708.02 (VIII).

The Applicants prepared this Petition in order to satisfy the requirements of 37 C.F.R. §1.102(d) and MPEP §708.02 (VIII). The pre-examination search required by these sections was "directed to the invention as claimed in the application for which special status is requested." MPEP §708.02 (VIII). The search performed in support of this Petition is believed to be in full compliance with the requirements of MPEP §708.02 (VIII); however, Applicants make no representation that the search covered every conceivable search area that might contain relevant prior art. It is always possible that prior art of greater relevance to the claims may exist. The Applicants urge the Examiner to conduct his or her own complete search of the prior art, and to thoroughly examine this application in view of the prior art cited above and any other prior art that may be located by the Examiner's independent search.

Further, while the Applicants have identified and discussed certain portions of each cited reference in order to satisfy the requirement for a "detailed discussion of the references, which discussion points out, with the particularly required by 37 C.F.R. §1.111(b) and (c), how the claimed subject matter is patentable over the references" (MPEP §708.02(VIII)), the Examiner should not limit review of these documents to the identified portions, but rather is urged to review and consider the entirety of each reference.

Respectfully submitted,

Colin D. Barnitz
Registration No. 35,061

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 Diagonal Rd., Suite 370
Alexandria, Virginia 22314
703-684-1120
Date: February 8, 2005